SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 01 June 2022

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-29361	Improper parsing of HTTP requests in Pallets Werkzeug v2.1.0 and below allows attackers to perform HTTP Request Smuggling using a crafted HTTP request with multiple requests included inside the body. NOTE: the vendor's position is that this behavior can only occur in unsupported configurations involving development mode and an HTTP server from outside the Werkzeug project	9.8	More Details
CVE-2022-26708	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.4. An attacker may be able to cause unexpected application termination or arbitrary code execution.	9.8	More Details
CVE-2022-26945	go-getter up to 1.5.11 and 2.0.2 allowed protocol switching, endless redirect, and configuration bypass via abuse of custom HTTP response header processing. Fixed in 1.6.1 and 2.1.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33016	An attacker can gain full access (read/write/delete) to sensitive folders due to hard-coded credentials on KUKA KR C4 control software for versions prior to 8.7 or any product running KSS.	9.8	More Details
CVE-2022-21831	A code injection vulnerability exists in the Active Storage >= v5.2.0 that could allow an attacker to execute code via image_processing arguments.	9.8	More Details
CVE-2022-30493	In oretnom23 Automotive Shop Management System v1.0, the product id parameter suffers from a blind SQL Injection Vulnerability allowing remote attackers to dump all database credential and gain admin access(privilege escalation).	9.8	More Details
CVE-2022-30495	In oretnom23 Automotive Shop Management System v1.0, the name id parameter is vulnerable to IDOR - Broken Access Control allowing attackers to change the admin password(vertical privilege escalation)	9.8	More Details
CVE-2022-30516	In Hospital-Management-System v1.0, the editid parameter in the doctor.php page is vulnerable to SQL injection attacks.	9.8	More Details
CVE-2022-26711	An integer overflow issue was addressed with improved input validation. This issue is fixed in tvOS 15.5, iTunes 12.12.4 for Windows, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	9.8	More Details
CVE-2022-30476	Tenda AC Series Router AC18_V15.03.05.19(6318) was discovered to contain a stack-based buffer overflow in the httpd module when handling /goform/SetFirewallCfg request.	9.8	More Details
CVE-2022-26723	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.4, macOS Big Sur 11.6.6. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution.	9.8	More Details
CVE-2022-26775	An integer overflow was addressed with improved input validation. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4. An attacker may be able to cause unexpected application termination or arbitrary code execution.	9.8	More Details
CVE-2022-26776	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.4, macOS Big Sur 11.6.6. An attacker may be able to cause unexpected application termination or arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29632	An arbitrary file upload vulnerability in the component /course/api/upload/pic of Roncoo Education v9.0.0 allows attackers to execute arbitrary code via a crafted file.	9.8	More Details
CVE-2022-29633	An access control issue in Linglong v1.0 allows attackers to access the background of the application via a crafted cookie.	9.8	More Details
CVE-2022-1556	The StaffList WordPress plugin before 3.1.5 does not properly sanitise and escape a parameter before using it in a SQL statement when searching for Staff in the admin dashboard, leading to an SQL Injection	9.8	More Details
CVE-2022-30477	Tenda AC Series Router AC18_V15.03.05.19(6318) was discovered to contain a stack-based buffer overflow in the httpd module when handling /goform/SetClientState request.	9.8	More Details
CVE-2022-30500	Jfinal cms 5.1.0 is vulnerable to SQL Injection.	9.8	More Details
CVE-2022-30474	Tenda AC Series Router AC18_V15.03.05.19(6318) was discovered to contain a heap overflow in the httpd module when handling /goform/saveParentControlInfo request.	9.8	More Details
CVE-2022-29650	Online Food Ordering System v1.0 was discovered to contain a SQL injection vulnerability via the Search parameter at /online-food-order/food-search.php.	9.8	More Details
CVE-2022-28862	In Archibus Web Central before 26.2, multiple SQL Injection vulnerabilities occur in dwr/call/plaincall/workflow.runWorkflowRule.dwr. Through the injection of arbitrary SQL statements, a potential attacker can modify query syntax and perform unauthorized (and unexpected) operations against the remote database. This is fixed in all recent versions, such as version 26.2.	9.8	More Details
CVE-2022-29660	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the id parameter at /admin.php/pic/admin/pic/del.	9.8	More Details
CVE-2022-1664	Dpkg::Source::Archive in dpkg, the Debian package management system, before version 1.21.8, 1.20.10, 1.19.8, 1.18.26 is prone to a directory traversal vulnerability. When extracting untrusted source packages in v2 and v3 source package formats that include a debian.tar, the in-place extraction can lead to directory traversal situations on specially crafted orig.tar and debian.tar tarballs.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30595	libImaging/TgaRleDecode.c in Pillow 9.1.0 has a heap buffer overflow in the processing of invalid TGA image files.	9.8	More Details
CVE-2022-30472	Tenda AC Seris Router AC18_V15.03.05.19(6318) has a stack-based buffer overflow vulnerability in function fromAddressNat	9.8	More Details
CVE-2022-29379	Nginx NJS v0.7.3 was discovered to contain a stack overflow in the function njs_default_module_loader at /src/njs/src/njs_module.c. NOTE: multiple third parties dispute this report, e.g., the behavior is only found in unreleased development code that was not part of the 0.7.2, 0.7.3, or 0.7.4 release	9.8	More Details
CVE-2022-23775	TrueStack Direct Connect 1.4.7 has Incorrect Access Control.	9.8	More Details
CVE-2022-24422	Dell iDRAC9 versions 5.00.00.00 and later but prior to 5.10.10.00, contain an improper authentication vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to gain access to the VNC Console.	9.6	More Details
CVE-2022-30584	Archer Platform 6.3 before 6.11 (6.11.0.0) contains an Improper Access Control Vulnerability within SSO ADFS functionality that could potentially be exploited by malicious users to compromise the affected system. 6.10 P3 (6.10.0.3) and 6.9 SP3 P4 (6.9.3.4) are also fixed releases.	9.6	More Details
CVE-2022-26833	An improper authentication vulnerability exists in the REST API functionality of Open Automation Software OAS Platform V16.00.0121. A specially-crafted series of HTTP requests can lead to unauthenticated use of the REST API. An attacker can send a series of HTTP requests to trigger this vulnerability.	9.4	More Details
CVE-2021-32989	When a non-existent resource is requested, the LCDS LAquis SCADA application (version 4.3.1.1011 and prior) returns error messages which may allow reflected cross-site scripting.	9.3	More Details
CVE-2022-31003	Sofia-SIP is an open-source Session Initiation Protocol (SIP) User-Agent library. Prior to version 1.13.8, when parsing each line of a sdp message, `rest = record + 2` will access the memory behind `\0` and cause an out-of-bounds write. An attacker can send a message with evil sdp to FreeSWITCH, causing a crash or more serious consequence, such as remote code execution. Version 1.13.8 contains a patch for this issue.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26082	A file write vulnerability exists in the OAS Engine SecureTransferFiles functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.	9.1	More Details
CVE-2021-27779	VersionVault Express exposes sensitive information that an attacker can use to impersonate the server or eavesdrop on communications with the server.	9.1	More Details
CVE-2022-26694	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.4. A plug-in may be able to inherit the application's permissions and access user data.	9.1	More Details
CVE-2022-26693	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.4. A plug-in may be able to inherit the application's permissions and access user data.	9.1	More Details
CVE-2022-1899	Out-of-bounds Read in GitHub repository radareorg/radare2 prior to 5.7.0.	9.1	More Details
CVE-2022-31013	Chat Server is the chat server for Vartalap, an open-source messaging application. Versions 2.3.2 until 2.6.0 suffer from a bug in validating the access token, resulting in authentication bypass. The function `this.authProvider.verifyAccessKey` is an async function, as the code is not using `await` to wait for the verification result. Every time the function responds back with success, along with an unhandled exception if the token is invalid. A patch is available in version 2.6.0.	9.1	More Details
CVE-2022-26857	Dell OpenManage Enterprise Versions 3.8.3 and prior contain an improper authorization vulnerability. A remote authenticated malicious user with low privileges may potentially exploit this vulnerability to bypass blocked functionalities and perform unauthorized actions.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-31265	The replay feature in the client in Wargaming World of Warships 0.11.4 allows remote attackers to execute code when a user launches a replay from an untrusted source.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26748	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-29685	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/User/level_sort.	8.8	More Details
CVE-2022-29664	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the id parameter at /admin.php/pic/admin/type/pl_save.	8.8	More Details
CVE-2021-33014	An attacker can gain VxWorks Shell after login due to hard-coded credentials on a KUKA KR C4 control software for versions prior to 8.7 or any product running KSS.	8.8	More Details
CVE-2021-40317	Piwigo 11.5.0 is affected by a SQL injection vulnerability via admin.php and the id parameter.	8.8	More Details
CVE-2022-1611	The Bulk Page Creator WordPress plugin before 1.1.4 does not protect its page creation functionalities with nonce checks, which makes them vulnerable to CSRF.	8.8	More Details
CVE-2022-29669	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the id parameter at /admin.php/news/admin/lists/zhuan.	8.8	More Details
CVE-2022-27305	Gibbon v23 does not generate a new session ID cookie after a user authenticates, making the application vulnerable to session fixation.	8.8	More Details
CVE-2022-29667	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via /admin.php/pic/admin/pic/hy. This vulnerability is exploited via restoring deleted photos.	8.8	More Details
CVE-2022-1808	Execution with Unnecessary Privileges in GitHub repository polonel/trudesk prior to 1.2.3.	8.8	More Details
CVE-2022-1883	SQL Injection in GitHub repository camptocamp/terraboard prior to 2.2.0.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30321	go-getter up to 1.5.11 and 2.0.2 allowed arbitrary host access via go-getter path traversal, symlink processing, and command injection flaws. Fixed in 1.6.1 and 2.1.0.	8.6	More Details
CVE-2022-30323	go-getter up to 1.5.11 and 2.0.2 panicked when processing password-protected ZIP files. Fixed in 1.6.1 and 2.1.0.	8.6	More Details
CVE-2022-30322	go-getter up to 1.5.11 and 2.0.2 allowed asymmetric resource exhaustion when go-getter processed malicious HTTP responses. Fixed in 1.6.1 and 2.1.0.	8.6	More Details
CVE-2021-44719	Docker Desktop 4.3.0 has Incorrect Access Control.	8.4	More Details
CVE-2022-25878	The package protobufjs before 6.11.3 are vulnerable to Prototype Pollution which can allow an attacker to add/modify properties of the Object.prototype. This vulnerability can occur in multiple ways: 1. by providing untrusted user input to util.setProperty or to ReflectionObject.setParsedOption functions 2. by parsing/loading .proto files	8.2	More Details
CVE-2021-32997	The affected Baker Hughes Bentley Nevada products (3500 System 1 6.x, Part No. 3060/00 versions 6.98 and prior, 3500 System 1, Part No. 3071/xx & 3072/xx versions 21.1 HF1 and prior, 3500 Rack Configuration, Part No. 129133-01 versions 6.4 and prior, and 3500/22M Firmware, Part No. 288055-01 versions 5.05 and prior) utilize a weak encryption algorithm for storage and transmission of sensitive data, which may allow an attacker to more easily obtain credentials used for access.	8.2	More Details
CVE-2022-1908	Buffer Over-read in GitHub repository bfabiszewski/libmobi prior to 0.11.	8.1	More Details
CVE-2022-22576	An improper authentication vulnerability exists in curl 7.33.0 to and including 7.82.0 which might allow reuse OAUTH2-authenticated connections without properly making sure that the connection was authenticated with the same credentials as set for this transfer. This affects SASL-enabled protocols: SMPTP(S), IMAP(S), POP3(S) and LDAP(S) (openldap only).	8.1	More Details
CVE-2022-1907	Buffer Over-read in GitHub repository bfabiszewski/libmobi prior to 0.11.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1931	Incorrect Synchronization in GitHub repository polonel/trudesk prior to 1.2.3.	8.1	More Details
CVE-2022-29248	Guzzle is a PHP HTTP client. Guzzle prior to versions 6.5.6 and 7.4.3 contains a vulnerability with the cookie middleware. The vulnerability is that it is not checked if the cookie domain equals the domain of the server which sets the cookie via the Set-Cookie header, allowing a malicious server to set cookies for unrelated domains. The cookie middleware is disabled by default, so most library consumers will not be affected by this issue. Only those who manually add the cookie middleware to the handler stack or construct the client with ['cookies' => true] are affected. Moreover, those who do not use the same Guzzle client to call multiple domains and have disabled redirect forwarding are not affected by this vulnerability. Guzzle versions 6.5.6 and 7.4.3 contain a patch for this issue. As a workaround, turn off the cookie middleware.	8.0	More Details
CVE-2022-30788	A crafted NTFS image can cause a heap-based buffer overflow in ntfs_mft_rec_alloc in NTFS-3G through 2021.8.22.	7.8	More Details
CVE-2022-1886	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-26769	A memory corruption issue was addressed with improved input validation. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26770	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26741	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26771	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 8.6, tvOS 15.5, iOS 15.5 and iPadOS 15.5. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26739	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.5, macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26772	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26774	A logic issue was addressed with improved state management. This issue is fixed in iTunes 12.12.4 for Windows. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2022-28394	EOL Product CVE - Installer of Trend Micro Password Manager (Consumer) versions 3.7.0.1223 and below provided by Trend Micro Incorporated contains an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries (CWE-427). Please note that this was reported on an EOL version of the product, and users are advised to upgrade to the latest supported version (5.x).	7.8	More Details
CVE-2022-30789	A crafted NTFS image can cause a heap-based buffer overflow in ntfs_check_log_client_array in NTFS-3G through 2021.8.22.	7.8	More Details
CVE-2022-30784	A crafted NTFS image can cause heap exhaustion in ntfs_get_attribute_value in NTFS-3G through 2021.8.22.	7.8	More Details
CVE-2022-1882	A use-after-free flaw was found in the Linux kernel's pipes functionality in how a user performs manipulations with the pipe post_one_notification() after free_pipe_info() that is already called. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2022-26738	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.5, macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-29637	An arbitrary file upload vulnerability in Mindoc v2.1-beta.5 allows attackers to execute arbitrary commands via a crafted Zip file.	7.8	More Details
CVE-2022-26737	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.5, macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30786	A crafted NTFS image can cause a heap-based buffer overflow in ntfs_names_full_collate in NTFS-3G through 2021.8.22.	7.8	More Details
CVE-2022-26742	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-22675	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.5, watchOS 8.6, macOS Big Sur 11.6.6, macOS Monterey 12.3.1, iOS 15.4.1 and iPadOS 15.4.1. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited..	7.8	More Details
CVE-2022-22672	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 15.4 and iPadOS 15.4, Security Update 2022-003 Catalina, macOS Monterey 12.3, macOS Big Sur 11.6.5. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26751	A memory corruption issue was addressed with improved input validation. This issue is fixed in iTunes 12.12.4 for Windows, iOS 15.5 and iPadOS 15.5, Security Update 2022-004 Catalina, macOS Big Sur 11.6.6, macOS Monterey 12.4. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2022-26747	This issue was addressed with improved checks. This issue is fixed in Xcode 13.4. An app may be able to gain elevated privileges.	7.8	More Details
CVE-2022-26744	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 15.5 and iPadOS 15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26749	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26750	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26722	A memory initialization issue was addressed. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to gain root privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26721	A memory initialization issue was addressed. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2022-26720	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26718	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.4, macOS Big Sur 11.6.6. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2022-26736	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.5, macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26714	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, Security Update 2022-004 Catalina, watchOS 8.6, macOS Big Sur 11.6.6, macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26768	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.4, watchOS 8.6, tvOS 15.5, macOS Big Sur 11.6.6. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26752	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26753	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26704	A validation issue existed in the handling of symlinks and was addressed with improved validation of symlinks. This issue is fixed in macOS Monterey 12.4. An app may be able to gain elevated privileges.	7.8	More Details
CVE-2022-26754	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26702	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 8.6, tvOS 15.5, iOS 15.5 and iPadOS 15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26756	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26757	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, Security Update 2022-004 Catalina, watchOS 8.6, macOS Big Sur 11.6.6, macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26761	A memory corruption issue was addressed with improved memory handling. This issue is fixed in Security Update 2022-004 Catalina, macOS Big Sur 11.6.6. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-26763	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, Security Update 2022-004 Catalina, watchOS 8.6, macOS Big Sur 11.6.6, macOS Monterey 12.4. A malicious application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2022-26715	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2022-26740	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.5, macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-1934	Use After Free in GitHub repository mruby/mruby prior to 3.2.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31011	TiDB is an open-source NewSQL database that supports Hybrid Transactional and Analytical Processing (HTAP) workloads. Under certain conditions, an attacker can construct malicious authentication requests to bypass the authentication process, resulting in privilege escalation or unauthorized access. Only users using TiDB 5.3.0 are affected by this vulnerability. TiDB version 5.3.1 contains a patch for this issue. Other mitigation strategies include turning off Security Enhanced Mode (SEM), disabling local login for non-root accounts, and ensuring that the same IP cannot be logged in as root and normal user at the same time.	7.8	More Details
CVE-2022-1927	Buffer Over-read in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-1897	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-1851	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-30700	An incorrect permission assignment vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to load a DLL with escalated privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2022-30701	An uncontrolled search path element vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to craft a special configuration file to load an untrusted library with escalated privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2022-1898	Use After Free in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-1942	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24414	Dell EMC CloudLink 7.1.3 and all earlier versions, Auth Token is exposed in GET requests. These request parameters can get logged in reverse proxies and server logs. Attackers may potentially use these tokens to access CloudLink server. Tokens should not be used in request URL to avoid such attacks.	7.6	More Details
CVE-2021-3555	A Buffer Overflow vulnerability in the RSTP server component of Eufy Indoor 2K Indoor Camera allows a local attacker to achieve remote code execution. This issue affects: Eufy Indoor 2K Indoor Camera 2.0.9.3 version and prior versions.	7.6	More Details
CVE-2022-26077	A cleartext transmission of sensitive information vulnerability exists in the OAS Engine configuration communications functionality of Open Automation Software OAS Platform V16.00.0112. A targeted network sniffing attack can lead to a disclosure of sensitive information. An attacker can sniff network traffic to trigger this vulnerability.	7.5	More Details
CVE-2022-29721	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/jobfairol/resumelist.	7.5	More Details
CVE-2022-30475	Tenda AC Series Router AC18_V15.03.05.19(6318) was discovered to contain a stack-based buffer overflow in the httpd module when handling /goform/WifiExtraSet request.	7.5	More Details
CVE-2022-26303	An external config control vulnerability exists in the OAS Engine SecureAddUser functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted series of network requests can lead to the creation of an OAS user account. An attacker can send a sequence of requests to trigger this vulnerability.	7.5	More Details
CVE-2022-26043	An external config control vulnerability exists in the OAS Engine SecureAddSecurity functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted series of network requests can lead to the creation of a custom Security Group. An attacker can send a sequence of requests to trigger this vulnerability.	7.5	More Details
CVE-2021-42860	A stack buffer overflow exists in Mini-XML v3.2. When inputting an unformed XML string to the mxmlLoadString API, it will cause a stack-buffer-overflow in mxml_string_getc:2611. NOTE: it is unclear whether this input is allowed by the API specification	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27169	An information disclosure vulnerability exists in the OAS Engine SecureBrowseFile functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted network request can lead to a disclosure of sensitive information. An attacker can send a network request to trigger this vulnerability.	7.5	More Details
CVE-2021-42859	A memory leak issue was discovered in Mini-XML v3.2 that could cause a denial of service. NOTE: testing reports are inconsistent, with some testers seeing the issue in both the 3.2 release and in the October 2021 development code, but others not seeing the issue in the 3.2 release	7.5	More Details
CVE-2022-22673	This issue was addressed with improved checks. This issue is fixed in iOS 15.5 and iPadOS 15.5. Processing a large input may lead to a denial of service.	7.5	More Details
CVE-2022-29720	74cmsSE v3.5.1 was discovered to contain an arbitrary file read vulnerability via the component \index\controller\Download.php.	7.5	More Details
CVE-2022-1589	The Change wp-admin login WordPress plugin before 1.1.0 does not properly check for authorisation and is also missing CSRF check when updating its settings, which could allow unauthenticated users to change the settings. The attacked could also be performed via a CSRF vector	7.5	More Details
CVE-2022-26701	A race condition was addressed with improved locking. This issue is fixed in tvOS 15.5, macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. An application may be able to execute arbitrary code with kernel privileges.	7.5	More Details
CVE-2022-26026	A denial of service vulnerability exists in the OAS Engine SecureConfigValues functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted network request can lead to loss of communications. An attacker can send a network request to trigger this vulnerability.	7.5	More Details
CVE-2022-30428	In ginadmin through 05-10-2022, the incoming path value is not filtered, resulting in arbitrary file reading.	7.5	More Details
CVE-2022-30427	In ginadmin through 05-10-2022 the incoming path value is not filtered, resulting in directory traversal.	7.5	More Details
CVE-2022-24418	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24417	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.	7.5	More Details
CVE-2022-23082	In CureKit versions v1.0.1 through v1.1.3 are vulnerable to path traversal as the function isFileOutsideDir fails to sanitize the user input which may lead to path traversal.	7.5	More Details
CVE-2022-31005	Vapor is an HTTP web framework for Swift. Users of Vapor prior to version 4.60.3 with FileMiddleware enabled are vulnerable to an integer overflow vulnerability that can crash the application. Version 4.60.3 contains a patch for this issue. As a workaround, disable FileMiddleware and serve via a Content Delivery Network.	7.5	More Details
CVE-2022-30473	Tenda AC Series Router AC18_V15.03.05.19(6318) has a stack-based buffer overflow vulnerability in function form_fast_setting_wifi_set	7.5	More Details
CVE-2022-31002	Sofia-SIP is an open-source Session Initiation Protocol (SIP) User-Agent library. Prior to version 1.13.8, an attacker can send a message with evil sdp to FreeSWITCH, which may cause a crash. This type of crash may be caused by a URL ending with `%`. Version 1.13.8 contains a patch for this issue.	7.5	More Details
CVE-2022-1815	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository jgraph/drawio prior to 18.1.2.	7.5	More Details
CVE-2022-31001	Sofia-SIP is an open-source Session Initiation Protocol (SIP) User-Agent library. Prior to version 1.13.8, an attacker can send a message with evil sdp to FreeSWITCH, which may cause crash. This type of crash may be caused by `#define MATCH(s, m) (strncmp(s, m, n = sizeof(m) - 1) == 0)`, which will make `n` bigger and trigger out-of-bound access when `IS_NON_WS(s[n])`. Version 1.13.8 contains a patch for this issue.	7.5	More Details
CVE-2022-29252	XWiki Platform Wiki UI Main Wiki is a package for managing subwikis. Starting with version 5.3-milestone-2, XWiki Platform Wiki UI Main Wiki contains a possible cross-site scripting vector in the `WikiManager.JoinWiki ` wiki page related to the "requestJoin" field. The issue is patched in versions 12.10.11, 14.0-rc-1, 13.4.7, and 13.10.3. The easiest available workaround is to edit the wiki page `WikiManager.JoinWiki` (with wiki editor) according to the suggestion provided in the GitHub Security Advisory.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29258	XWiki Platform Filter UI provides a generic user interface to convert from a XWiki Filter input stream to an output stream with settings for each stream. Starting with versions 6.0-milestone-2 and 5.4.4 and prior to versions 12.10.11, 14.0-rc-1, 13.4.7, and 13.10.3, XWiki Platform Filter UI contains a possible cross-site scripting vector in the `Filter.FilterStreamDescriptorForm` wiki page related to pretty much all the form fields printed in the home page of the application. The issue is patched in versions 12.10.11, 14.0-rc-1, 13.4.7, and 13.10.3. The easiest workaround is to edit the wiki page `Filter.FilterStreamDescriptorForm` (with wiki editor) according to the instructions in the GitHub Security Advisory.	7.4	More Details
CVE-2022-29251	XWiki Platform Flamingo Theme UI is a tool that allows customization and preview of any Flamingo-based skin. Starting with versions 6.2.4 and 6.3-rc-1, a possible cross-site scripting vector is present in the `FlamingoThemesCode.WebHomeSheet` wiki page related to the "newThemeName" form field. The issue is patched in versions 12.10.11, 14.0-rc-1, 13.4.7, and 13.10.3. The easiest available workaround is to edit the wiki page `FlamingoThemesCode.WebHomeSheet` (with wiki editor) according to the suggestion provided in the GitHub Security Advisory.	7.4	More Details
CVE-2022-29651	An arbitrary file upload vulnerability in the Select Image function of Online Food Ordering System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-22127	Tableau is aware of a broken access control vulnerability present in Tableau Server affecting Tableau Server customers using Local Identity Store for managing users. The vulnerability allows a malicious site administrator to change passwords for users in different sites hosted on the same Tableau Server, resulting in the potential for unauthorized access to data.Tableau Server versions affected are:2020.4.16, 2021.1.13, 2021.2.10, 2021.3.9, 2021.4.4 and earlierNote: All future releases of Tableau Server will address this security issue. Versions that are no longer supported are not tested and may be vulnerable.	7.2	More Details
CVE-2022-29670	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the id parameter at /admin.php/pic/admin/type/del.	7.2	More Details
CVE-2022-29683	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/Label/page_del.	7.2	More Details
CVE-2022-29676	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the id parameter at /admin.php/pic/admin/lists/zhuan.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29662	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the id parameter at /admin.php/news/admin/news/save.	7.2	More Details
CVE-2022-29680	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/user/zu_del.	7.2	More Details
CVE-2022-29681	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/Links/del.	7.2	More Details
CVE-2022-29682	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/vod/admin/topic/del.	7.2	More Details
CVE-2022-29666	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the id parameter at /admin.php/pic/admin/lists/zhuan.	7.2	More Details
CVE-2022-29684	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/Label/js_del.	7.2	More Details
CVE-2022-29665	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the id parameter at /admin.php/news/admin/topic/save.	7.2	More Details
CVE-2022-29686	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/singer/admin/lists/zhuan.	7.2	More Details
CVE-2022-29687	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/user/level_del.	7.2	More Details
CVE-2022-29688	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/singer/admin/singer/hy.	7.2	More Details
CVE-2022-29663	CSCMS Music Portal System v4.2 was discovered to contain a SQL injection vulnerability via the id parameter at /admin.php/pic/admin/type/hy.	7.2	More Details
CVE-2022-29689	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/singer/admin/singer/del.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29661	CSCMS Music Portal System v4.2 was discovered to contain a blind SQL injection vulnerability via the id parameter at /admin.php/pic/admin/type/save.	7.2	More Details
CVE-2022-26697	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory.	7.1	More Details
CVE-2022-30687	Trend Micro Maximum Security 2022 is vulnerable to a link following vulnerability that could allow a low privileged local user to manipulate the product's secure erase feature to delete arbitrary files.	7.1	More Details
CVE-2022-26773	A logic issue was addressed with improved state management. This issue is fixed in iTunes 12.12.4 for Windows. An application may be able to delete files for which it does not have permission.	7.1	More Details
CVE-2022-21827	An improper privilege vulnerability has been discovered in Citrix Gateway Plug-in for Windows (Citrix Secure Access for Windows) <21.9.1.2 what could allow an attacker who has gained local access to a computer with Citrix Gateway Plug-in installed, to corrupt or delete files as SYSTEM.	7.1	More Details
CVE-2022-26698	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory.	7.1	More Details
CVE-2022-26743	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.4. An attacker that has already achieved code execution in macOS Recovery may be able to escalate to kernel privileges.	7.0	More Details
CVE-2021-28508	This advisory documents the impact of an internally found vulnerability in Arista EOS state streaming telemetry agent TerminAttr and OpenConfig transport protocols. The impact of this vulnerability is that, in certain conditions, TerminAttr might leak IPsec sensitive data in clear text in CVP to other authorized users, which could cause IPsec traffic to be decrypted or modified by other authorized users on the device.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21951	A Cleartext Transmission of Sensitive Information vulnerability in SUSE Rancher, Rancher allows attackers on the network to read and change network data due to missing encryption of data transmitted via the network when a cluster is created from an RKE template with the CNI value overridden This issue affects: SUSE Rancher Rancher versions prior to 2.5.14; Rancher versions prior to 2.6.5.	6.8	More Details
CVE-2021-27783	User generated PPKG file for Bulk Enroll may have unencrypted sensitive information exposed.	6.8	More Details
CVE-2022-29402	TP-Link TL-WR840N EU v6.20 was discovered to contain insecure protections for its UART console. This vulnerability allows attackers to connect to the UART port via a serial connection and execute commands as the root user without authentication.	6.8	More Details
CVE-2022-26865	Dell Support Assist OS Recovery versions before 5.5.2 contain an Authentication Bypass vulnerability. An unauthenticated attacker with physical access to the system may exploit this vulnerability by bypassing OS Recovery authentication in order to run arbitrary code on the system as Administrator.	6.8	More Details
CVE-2022-30785	A file handle created in fuse_lib_opendir, and later used in fuse_lib_readdir, enables arbitrary memory read and write operations in NTFS-3G through 2021.8.22 when using libfuse-lite.	6.7	More Details
CVE-2022-26691	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2022-003 Catalina, macOS Monterey 12.3, macOS Big Sur 11.6.5. An application may be able to gain elevated privileges.	6.7	More Details
CVE-2022-30787	An integer underflow in fuse_lib_readdir enables arbitrary memory read operations in NTFS-3G through 2021.8.22 when using libfuse-lite.	6.7	More Details
CVE-2022-30783	An invalid return code in fuse_kern_mount enables intercepting of libfuse-lite protocol traffic between NTFS-3G and the kernel in NTFS-3G through 2021.8.22 when using libfuse-lite.	6.7	More Details
CVE-2021-27781	The Master operator may be able to embed script tag in HTML with alert pop-up display cookie.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29245	SSH.NET is a Secure Shell (SSH) library for .NET. In versions 2020.0.0 and 2020.0.1, during an `X25519` key exchange, the client's private key is generated with `System.Random`. `System.Random` is not a cryptographically secure random number generator, it must therefore not be used for cryptographic purposes. When establishing an SSH connection to a remote host, during the X25519 key exchange, the private key is generated with a weak random number generator whose seed can be brute forced. This allows an attacker who is able to eavesdrop on the communications to decrypt them. Version 2020.0.2 contains a patch for this issue. As a workaround, one may disable support for `curve25519-sha256` and `curve25519-sha256@libssh.org` key exchange algorithms.	6.5	More Details
CVE-2022-29220	github-action-merge-dependabot is an action that automatically approves and merges dependabot pull requests (PRs). Prior to version 3.2.0, github-action-merge-dependabot does not check if a commit created by dependabot is verified with the proper GPG key. There is just a check if the actor is set to `dependabot[bot]` to determine if the PR is a legit PR. Theoretically, an owner of a seemingly valid and legit action in the pipeline can check if the PR is created by dependabot and if their own action has enough permissions to modify the PR in the pipeline. If so, they can modify the PR by adding a second seemingly valid and legit commit to the PR, as they can set arbitrarily the username and email in for commits in git. Because the bot only checks if the actor is valid, it would pass the malicious changes through and merge the PR automatically, without getting noticed by project maintainers. It would probably not be possible to determine where the malicious commit came from, as it would only say `dependabot[bot]` and the corresponding email-address. Version 3.2.0 contains a patch for this issue.	6.5	More Details
CVE-2022-22361	IBM Business Automation Workflow traditional 21.0.1 through 21.0.3, 20.0.0.1 through 20.0.0.2, 19.0.0.1 through 19.0.0.3, 18.0.0.0 through 18.0.0.1, IBM Business Automation Workflow containers V21.0.1 - V21.0.3 20.0.0.1 through 20.0.0.2, IBM Business Process Manager 8.6.0.0 through 8.6.0.201803, and 8.5.0.0 through 8.5.0.201706 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	6.5	More Details
CVE-2022-30585	The REST API in Archer Platform 6.x before 6.11 (6.11.0.0) contains an Authorization Bypass Vulnerability. A remote authenticated malicious user could potentially exploit this vulnerability to view sensitive information. 6.10 P3 (6.10.0.3) and 6.9 SP3 P4 (6.9.3.4) are also fixed releases.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1947	Use of Incorrect Operator in GitHub repository polonel/trudesk prior to 1.2.3.	6.5	More Details
CVE-2022-1583	The External Links in New Window / New Tab WordPress plugin before 1.43 does not ensure window.opener is set to "null" when links to external sites are clicked, which may enable tabnabbing attacks to occur.	6.5	More Details
CVE-2022-31015	Waitress is a Web Server Gateway Interface server for Python 2 and 3. Waitress versions 2.1.0 and 2.1.1 may terminate early due to a thread closing a socket while the main thread is about to call select(). This will lead to the main thread raising an exception that is not handled and then causing the entire application to be killed. This issue has been fixed in Waitress 2.1.2 by no longer allowing the WSGI thread to close the socket. Instead, that is always delegated to the main thread. There is no work-around for this issue. However, users using waitress behind a reverse proxy server are less likely to have issues if the reverse proxy always reads the full response.	6.5	More Details
CVE-2022-30508	DedeCMS v5.7.93 was discovered to contain arbitrary file deletion vulnerability in upload.php via the delete parameter.	6.5	More Details
CVE-2022-1348	A vulnerability was found in logrotate in how the state file is created. The state file is used to prevent parallel executions of multiple instances of logrotate by acquiring and releasing a file lock. When the state file does not exist, it is created with world-readable permission, allowing an unprivileged user to lock the state file, stopping any rotation. This flaw affects logrotate versions before 3.20.0.	6.5	More Details
CVE-2021-42692	There is a stack-overflow vulnerability in tinytoml v0.4 that can cause a crash or DoS.	6.5	More Details
CVE-2022-22662	A cookie management issue was addressed with improved state management. This issue is fixed in Security Update 2022-003 Catalina, macOS Big Sur 11.6.5. Processing maliciously crafted web content may disclose sensitive user information.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29256	sharp is an application for Node.js image processing. Prior to version 0.30.5, there is a possible vulnerability in logic that is run only at `npm install` time when installing versions of `sharp` prior to the latest v0.30.5. If an attacker has the ability to set the value of the `PKG_CONFIG_PATH` environment variable in a build environment then they might be able to use this to inject an arbitrary command at `npm install` time. This is not part of any runtime code, does not affect Windows users at all, and is unlikely to affect anyone that already cares about the security of their build environment. This problem is fixed in version 0.30.5.	6.5	More Details
CVE-2022-31620	In libjpeg before 1.64, BitStream<false>::Get in bitstream.hpp has an assertion failure that may cause denial of service. This is related to out-of-bounds array access during arithmetically coded lossless scan or arithmetically coded sequential scan.	6.5	More Details
CVE-2022-20821	A vulnerability in the health check RPM of Cisco IOS XR Software could allow an unauthenticated, remote attacker to access the Redis instance that is running within the NOSi container. This vulnerability exists because the health check RPM opens TCP port 6379 by default upon activation. An attacker could exploit this vulnerability by connecting to the Redis instance on the open port. A successful exploit could allow the attacker to write to the Redis in-memory database, write arbitrary files to the container filesystem, and retrieve information about the Redis database. Given the configuration of the sandboxed container that the Redis instance runs in, a remote attacker would be unable to execute remote code or abuse the integrity of the Cisco IOS XR Software host system.	6.5	More Details
CVE-2022-26726	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-004 Catalina, watchOS 8.6, macOS Monterey 12.4, macOS Big Sur 11.6.6. An app may be able to capture a user's screen.	6.5	More Details
CVE-2022-29405	In Apache Archiva, any registered user can reset password for any users. This is fixed in Archiva 2.2.8	6.5	More Details
CVE-2021-35487	Nokia Broadcast Message Center through 11.1.0 allows an authenticated user to perform a Boolean Blind SQL Injection attack on the endpoint /owui/block/send-receive-updates (for the Manage Alerts page) via the extIdentifier HTTP POST parameter. This allows an attacker to obtain the database user, database name, and database version information, and potentially database data.	6.5	More Details
CVE-2022-26755	This issue was addressed with improved environment sanitization. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to break out of its sandbox.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20671	Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-29359	A stored cross-site scripting (XSS) vulnerability in /scas/?page=clubs/application_form&id=7 of School Club Application System v0.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the firstname parameter.	6.1	More Details
CVE-2022-20666	Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-29710	A cross-site scripting (XSS) vulnerability in uploadConfirm.php of LimeSurvey v5.3.9 and below allows attackers to execute arbitrary web scripts or HTML via a crafted plugin.	6.1	More Details
CVE-2022-20667	Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20668	Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20669	Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20670	Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20673	Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20672	Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-20674	Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2022-31648	Talend Administration Center is vulnerable to a reflected Cross-Site Scripting (XSS) issue in the SSO login endpoint. The issue is fixed for versions 8.0.x in TPS-5233, for versions 7.3.x in TPS-5324, and for versions 7.2.x in TPS-5235. Earlier versions of Talend Administration Center may also be impacted; users are encouraged to update to a supported version.	6.1	More Details
CVE-2022-1009	The Smush WordPress plugin before 3.9.9 does not sanitise and escape a configuration parameter before outputting it back in an admin page when uploading a malicious preset configuration, leading to a Reflected Cross-Site Scripting. For the attack to be successful, an attacker would need an admin to upload a malicious configuration file	6.1	More Details
CVE-2022-1527	The WP 2FA WordPress plugin before 2.2.1 does not sanitise and escape a parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1528	The VikBooking Hotel Booking Engine & PMS WordPress plugin before 1.5.9 does not escape the current URL before putting it back in a JavaScript context, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1582	The External Links in New Window / New Tab WordPress plugin before 1.43 does not properly escape URLs it concatenates to onclick event handlers, which makes Stored Cross-Site Scripting attacks possible.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28509	This advisory documents the impact of an internally found vulnerability in Arista EOS state streaming telemetry agent TerminAttr and OpenConfig transport protocols. The impact of this vulnerability is that, in certain conditions, TerminAttr might leak MACsec sensitive data in clear text in CVP to other authorized users, which could cause MACsec traffic to be decrypted or modified by other authorized users on the device.	6.1	More Details
CVE-2022-29349	kkFileView v4.0.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the url parameter at /controller/OnlinePreviewController.java.	6.1	More Details
CVE-2022-22577	An XSS Vulnerability in Action Pack >= 5.2.0 and < 5.2.0 that could allow an attacker to bypass CSP for non HTML like responses.	6.1	More Details
CVE-2022-27777	A XSS Vulnerability in Action View tag helpers >= 5.2.0 and < 5.2.0 which would allow an attacker to inject content if able to control input into specific attributes.	6.1	More Details
CVE-2022-1678	An issue was discovered in the Linux Kernel from 4.18 to 4.19, an improper update of sock reference in TCP pacing can lead to memory/netns leak, which can be used by remote clients.	5.9	More Details
CVE-2022-1261	Matrikon, a subsidary of Honeywell Matrikon OPC Server (all versions) is vulnerable to a condition where a low privileged user allowed to connect to the OPC server to use the functions of the IPersisFile to execute operating system processes with system-level privileges.	5.8	More Details
CVE-2022-30973	We failed to apply the fix for CVE-2022-30126 to the 1.x branch in the 1.28.2 release. In Apache Tika, a regular expression in the StandardsText class, used by the StandardsExtractingContentHandler could lead to a denial of service caused by backtracking on a specially crafted file. This only affects users who are running the StandardsExtractingContentHandler, which is a non-standard handler. This is fixed in 1.28.3.	5.5	More Details
CVE-2022-26727	This issue was addressed with improved entitlements. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4. A malicious application may be able to modify protected parts of the file system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20797	A vulnerability in the web-based management interface of Cisco Secure Network Analytics, formerly Cisco Stealthwatch Enterprise, could allow an authenticated, remote attacker to execute arbitrary commands as an administrator on the underlying operating system. This vulnerability is due to insufficient user input validation by the web-based management interface of the affected software. An attacker could exploit this vulnerability by injecting arbitrary commands in the web-based management interface. A successful exploit could allow the attacker to make configuration changes on the affected device or cause certain services to restart unexpectedly.	5.5	More Details
CVE-2022-31651	In SoX 14.4.2, there is an assertion failure in rate_init in rate.c in libsox.a.	5.5	More Details
CVE-2022-31650	In SoX 14.4.2, there is a floating-point exception in lsx_aiffstartwrite in aiff.c in libsox.a.	5.5	More Details
CVE-2022-31624	MariaDB Server before 10.7 is vulnerable to Denial of Service. While executing the plugin/server_audit/server_audit.c method log_statement_ex, the held lock lock_bigbuffer is not released correctly, which allows local users to trigger a denial of service due to the deadlock.	5.5	More Details
CVE-2022-26724	An authentication issue was addressed with improved state management. This issue is fixed in tvOS 15.5. A local user may be able to enable iCloud Photos without authentication.	5.5	More Details
CVE-2022-22676	An event handler validation issue in the XPC Services API was addressed by removing the service. This issue is fixed in macOS Monterey 12.2. An application may be able to delete files for which it does not have permission.	5.5	More Details
CVE-2022-31621	MariaDB Server before 10.7 is vulnerable to Denial of Service. In extra/mariabackup/ds_xbstream.cc, when an error occurs (stream_ctxt->dest_file == NULL) while executing the method xbstream_open, the held lock is not released correctly, which allows local users to trigger a denial of service due to the deadlock. Note: The vendor argues this is just an improper locking bug and not a vulnerability with adverse effects.	5.5	More Details
CVE-2022-26706	An access issue was addressed with additional sandbox restrictions on third-party applications. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Big Sur 11.6.6, macOS Monterey 12.4. A sandboxed process may be able to circumvent sandbox restrictions.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26712	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to modify protected parts of the file system.	5.5	More Details
CVE-2022-31622	MariaDB Server before 10.7 is vulnerable to Denial of Service. In extra/mariabackup/ds_compress.cc, when an error occurs (pthread_create returns a nonzero value) while executing the method create_worker_threads, the held lock is not released correctly, which allows local users to trigger a denial of service due to the deadlock. Note: The vendor argues this is just an improper locking bug and not a vulnerability with adverse effects.	5.5	More Details
CVE-2022-31623	MariaDB Server before 10.7 is vulnerable to Denial of Service. In extra/mariabackup/ds_compress.cc, when an error occurs (i.e., going to the err label) while executing the method create_worker_threads, the held lock thd->ctrl_mutex is not released correctly, which allows local users to trigger a denial of service due to the deadlock. Note: The vendor argues this is just an improper locking bug and not a vulnerability with adverse effects.	5.5	More Details
CVE-2021-44974	radareorg radare2 version 5.5.2 is vulnerable to NULL Pointer Dereference via libr/bin/p/bin_symbols.c binary symbol parser.	5.5	More Details
CVE-2022-29358	epub2txt2 v2.04 was discovered to contain an integer overflow via the function bug in _parse_special_tag at sxmlc.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted XML file.	5.5	More Details
CVE-2022-26746	This issue was addressed by removing the vulnerable code. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to bypass Privacy preferences.	5.5	More Details
CVE-2022-22674	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Monterey 12.3.1, Security Update 2022-004 Catalina, macOS Big Sur 11.6.6. A local user may be able to read kernel memory.	5.5	More Details
CVE-2022-26728	This issue was addressed with improved entitlements. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to access restricted files.	5.5	More Details
CVE-2022-22616	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-003 Catalina, macOS Monterey 12.3, macOS Big Sur 11.6.5. A maliciously crafted ZIP archive may bypass Gatekeeper checks.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22663	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in iOS 15.4 and iPadOS 15.4, Security Update 2022-004 Catalina, macOS Monterey 12.3, macOS Big Sur 11.6.6. A malicious application may bypass Gatekeeper checks.	5.5	More Details
CVE-2022-26745	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.6.6. A malicious application may disclose restricted memory.	5.5	More Details
CVE-2022-26767	The issue was addressed with additional permissions checks. This issue is fixed in macOS Monterey 12.4, macOS Big Sur 11.6.6. A malicious application may be able to bypass Privacy preferences.	5.5	More Details
CVE-2022-26766	A certificate parsing issue was addressed with improved checks. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, Security Update 2022-004 Catalina, watchOS 8.6, macOS Big Sur 11.6.6, macOS Monterey 12.4. A malicious app may be able to bypass signature validation.	5.5	More Details
CVE-2022-20802	A vulnerability in the web interface of Cisco Enterprise Chat and Email (ECE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input that is processed by the web interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. A successful exploit could allow the attacker to execute arbitrary code in the context of the interface or access sensitive, browser-based information. To successfully exploit this vulnerability, an attacker would need valid agent credentials.	5.4	More Details
CVE-2022-1928	Cross-site Scripting (XSS) - Stored in GitHub repository go-gitea/gitea prior to 1.16.9.	5.4	More Details
CVE-2022-1909	Cross-site Scripting (XSS) - Stored in GitHub repository causefx/organizr prior to 2.1.2200.	5.4	More Details
CVE-2022-0642	The JivoChat Live Chat WordPress plugin before 1.3.5.4 does not properly check CSRF tokens on POST requests to the plugins admin page, and does not sanitise some parameters, leading to a stored Cross-Site Scripting vulnerability where an attacker can trick a logged in administrator to inject arbitrary javascript.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1562	The Enable SVG WordPress plugin before 1.4.0 does not sanitise uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads	5.4	More Details
CVE-2022-30494	In oretnom23 Automotive Shop Management System v1.0, the first and last name user fields suffer from a stored XSS Injection Vulnerability allowing remote attackers to gain admin access and view internal IPs.	5.4	More Details
CVE-2022-29362	A cross-site scripting (XSS) vulnerability in /navigation/create?ParentID=%23 of ZKEACMS v3.5.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the ParentID parameter.	5.4	More Details
CVE-2021-27780	The software may be vulnerable to both Un-Auth XML interaction and unauthenticated device enrollment.	5.3	More Details
CVE-2022-29091	Dell Unity, Dell UnityVSA, and Dell UnityXT versions prior to 5.2.0.0.5.173 contain a Reflected Cross-Site Scripting Vulnerability in Unisphere GUI. An Unauthenticated Remote Attacker could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	5.3	More Details
CVE-2021-34360	A cross-site request forgery (CSRF) vulnerability has been reported to affect QNAP device running Proxy Server. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Proxy Server: QTS 4.5.x: Proxy Server 1.4.2 (2021/12/30) and later QuTS hero h5.0.0: Proxy Server 1.4.3 (2022/01/18) and later QuTScloud c4.5.6: Proxy Server 1.4.2 (2021/12/30) and later	5.3	More Details
CVE-2022-26725	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.4. Photo location information may persist after it is removed with Preview Inspector.	5.3	More Details
CVE-2022-26067	An information disclosure vulnerability exists in the OAS Engine SecureTransferFiles functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted series of network requests can lead to arbitrary file read. An attacker can send a sequence of requests to trigger this vulnerability.	4.9	More Details
CVE-2022-1926	Integer Overflow or Wraparound in GitHub repository polonel/trudesk prior to 1.2.3.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31007	eLabFTW is an electronic lab notebook manager for research teams. Prior to version 4.3.0, a vulnerability allows an authenticated user with an administrator role in a team to assign itself system administrator privileges within the application, or create a new system administrator account. The issue has been corrected in eLabFTW version 4.3.0. In the context of eLabFTW, an administrator is a user account with certain privileges to manage users and content in their assigned team/teams. A system administrator account can manage all accounts, teams and edit system-wide settings within the application. The impact is not deemed as high, as it requires the attacker to have access to an administrator account. Regular user accounts cannot exploit this to gain admin rights. A workaround for one if the issues is removing the ability of administrators to create accounts.	4.9	More Details
CVE-2022-1643	The Birthdays Widget WordPress plugin through 1.7.18 does not sanitise and escape some of its fields, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1644	The Call&Book Mobile Bar WordPress plugin through 1.2.2 does not sanitize and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2022-1645	The Amazon Link WordPress plugin through 3.2.10 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2022-1646	The Simple Real Estate Pack WordPress plugin through 1.4.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1568	The Team Members WordPress plugin before 5.1.1 does not escape some of its Team settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-29380	Academy-LMS v4.3 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the SEO panel.	4.8	More Details
CVE-2022-1387	The No Future Posts WordPress plugin through 1.4 does not escape its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1566	The Quotes llama WordPress plugin before 1.0.0 does not sanitise and escape Quotes, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed. The attack could also be performed by tricking an admin to import a malicious CSV file	4.8	More Details
CVE-2022-1299	The Slideshow WordPress plugin through 2.3.1 does not sanitize and escape some of its default slideshow settings, which could allow high-privileged users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1564	The Form Maker by 10Web WordPress plugin before 1.14.12 does not sanitize and escape the Custom Text settings, which could allow high privilege user such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-0376	The User Meta WordPress plugin before 2.4.3 does not sanitise and escape the Form Name, as well as Shared Field Labels before outputting them in the admin dashboard when editing a form, which could allow high privilege users to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-1275	The BannerMan WordPress plugin through 0.2.4 does not sanitize or escape its settings, which could allow high-privileged users to perform Cross-Site Scripting attacks when the unfiltered_html is disallowed (such as in multisite)	4.8	More Details
CVE-2022-1294	The IMDB info box WordPress plugin through 2.0 does not sanitize and escape some of its settings, which could allow high-privileged users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-20765	A vulnerability in the web applications of Cisco UCS Director could allow an authenticated, remote attacker to conduct a cross-site scripting attack on an affected system. This vulnerability is due to unsanitized user input. An attacker could exploit this vulnerability by submitting custom JavaScript to affected web applications. A successful exploit could allow the attacker to rewrite web page content, access sensitive information stored in the applications, and alter data by submitting forms.	4.8	More Details
CVE-2022-1395	The Easy FAQ with Expanding Text WordPress plugin through 3.2.8.3.1 does not sanitise and escape its settings, allowing high privilege users to perform Cross-Site Scripting attacks when unfiltered_html is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1456	The Poll Maker WordPress plugin before 4.0.2 does not sanitise and escape some settings, which could allow high privilege users such as admin to perform Store Cross-Site Scripting attack even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-1542	The HPB Dashboard WordPress plugin through 1.3.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2022-26765	A race condition was addressed with improved state handling. This issue is fixed in watchOS 8.6, tvOS 15.5, macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.	4.7	More Details
CVE-2022-26764	A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.6, tvOS 15.5, macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	4.7	More Details
CVE-2022-29408	Persistent Cross-Site Scripting (XSS) vulnerability in Vsourz Digital's Advanced Contact form 7 DB plugin <= 1.8.7 at WordPress.	4.7	More Details
CVE-2022-26690	Description: A race condition was addressed with additional validation. This issue is fixed in macOS Monterey 12.3. A malicious application may be able to modify protected parts of the file system.	4.7	More Details
CVE-2022-1893	Improper Removal of Sensitive Information Before Storage or Transfer in GitHub repository polonel/trudesk prior to 1.2.3.	4.6	More Details
CVE-2022-26688	An issue in the handling of symlinks was addressed with improved validation. This issue is fixed in Security Update 2022-003 Catalina, macOS Monterey 12.3, macOS Big Sur 11.6.5. A malicious app with root privileges may be able to modify the contents of system files.	4.4	More Details
CVE-2022-20806	Multiple vulnerabilities in the API and web-based management interfaces of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker to write files or disclose sensitive information on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20809	Multiple vulnerabilities in the API and web-based management interfaces of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker to write files or disclose sensitive information on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	4.3	More Details
CVE-2022-28875	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant and in certain WithSecure products whereby the scanning the aemobile component can crash the scanning engine. The exploit can be triggered remotely by an attacker.	4.3	More Details
CVE-2022-29243	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Prior to versions 22.2.7 and 23.0.4, missing input-size validation of new session names allows users to create app passwords with long names. These long names are then loaded into memory on usage, resulting in impacted performance. Versions 22.2.7 and 23.0.4 contain a fix for this issue. There are currently no known workarounds available.	4.3	More Details
CVE-2022-26731	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. A malicious website may be able to track users in Safari private browsing mode.	4.3	More Details
CVE-2022-1203	The Content Mask WordPress plugin before 1.8.4.1 does not have authorisation and CSRF checks in various AJAX actions, as well as does not validate the option to be updated to ensure it belongs to the plugin. As a result, any authenticated user, such as subscriber could modify arbitrary blog options	4.3	More Details
CVE-2022-20807	Multiple vulnerabilities in the API and web-based management interfaces of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker to write files or disclose sensitive information on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	4.3	More Details
CVE-2021-32966	Philips Interoperability Solution XDS versions 2.5 through 3.11 and 2018-1 through 2021-1 are vulnerable to clear text transmission of sensitive information when configured to use LDAP via TLS and where the domain controller returns LDAP referrals, which may allow an attacker to remotely read LDAP system credentials.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29082	Dell EMC NetWorker versions 19.1.x, 19.1.0.x, 19.1.1.x, 19.2.x, 19.2.0.x, 19.2.1.x 19.3.x, 19.3.0.x, 19.4.x, 19.4.0.x, 19.5.x,19.5.0.x, 19.6 and 19.6.0.1 and 19.6.0.2 contain an Improper Validation of Certificate with Host Mismatch vulnerability in Rabbitmq port 5671 which could allow remote attackers to spoof certificates.	3.7	More Details
CVE-2021-4231	A vulnerability was found in Angular up to 11.0.4/11.1.0-next.2. It has been classified as problematic. Affected is the handling of comments. The manipulation leads to cross site scripting. It is possible to launch the attack remotely but it might require an authentication first. Upgrading to version 11.0.5 and 11.1.0-next.3 is able to address this issue. The name of the patch is ba8da742e3b243e8f43d4c63aa842b44e14f2b09. It is recommended to upgrade the affected component.	3.5	More Details
CVE-2021-4232	A vulnerability classified as problematic has been found in Zoo Management System 1.0. Affected is an unknown function of the file admin/manage-ticket.php. The manipulation with the input <script>alert(1) </script> leads to cross site scripting. It is possible to launch the attack remotely.	3.5	More Details
CVE-2022-29253	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting with version 8.3-rc-1 and prior to versions 12.10.3 and 14.0, one can ask for any file located in the classloader using the template API and a path with ".." in it. The issue is patched in versions 14.0 and 13.10.3. There is no easy workaround for this issue.	2.7	More Details
CVE-2022-26703	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.5 and iPadOS 15.5. A person with physical access to an iOS device may be able to access photos from the lock screen.	2.4	More Details